UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,681	02/06/2004	Pradeep Bahl	M1103.70234US00	7805

45840 7590 04/26/2010

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
HUSSAIN, TAUQIR	

ART UNIT	PAPER NUMBER
2452	

MAIL DATE	DELIVERY MODE
04/26/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/773,681	BAHL ET AL.	
	Examiner	Art Unit	
	TAUQIR HUSSAIN	2452	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,14,16,18-23 and 25-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,14,16,18-23 and 25-45* is/are rejected.

7)☒ Claim(s) *46 and 47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/22/2010 has been entered.

Response to Amendment

2. This office action is in response to amendment /reconsideration filed on 01/22/2010, the amendment/reconsideration has been considered. Claims 1, 16, 22 and 40 have been amended; claims 13 and 15 have been canceled and claims 46-47 are newly added. Therefore, claims 1-10, 14, 16, 18-23 and 25-47 are pending for examination, the rejection cited as stated below.

Response to Arguments

3. Applicant's arguments filed on 01/22/2010 have been fully considered but they are not deemed to be persuasive. In the remarks, applicant argued in substance that

(a) Prior art "Tezuka, Mayer and Jemes" does not teach "the network species component indicating a network species classification selected from among a plurality of network species classification, the plurality of network species classification including an enterprise network, a home network and a public place network".

As to point (a), Examiner respectfully submit that arguments have been moot in view of new grounds of rejection. Ayyagari has been introduced as the primary art which discloses the above limitation in Ayyagari, Fig.5, [0045], where “sys tray” icon contains the available plurality of networks which is same as network species classification, since it shows all the available/classifies network to a user in order for user to make a selection and [0036], where using a zero configuration system within itself determines according to the policies setup without user intervention and so zero configuration recognizes the network species by determining whether user is at home, at work, in transit, at the airport or in a hotel with available network e.g. WAN GPRS, 802.1x, WLAN 2, STA and this implementation is defined in [0035] which incorporates, "just works" user experience, which greatly enhances the ability to realize the benefits of true nomadic computing. In this way, a wireless computer user may work on an established network at home, at work, in transit, at the airport, in a hotel, etc., and may form ad hoc wireless networks with other wireless users all without having to manually reconfigure or adjust network variable settings to enable association with the different network types.

Similar rationale applies to the limitations discussed for claims 22 and 40 in remarks see pages 18-19.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

5. Claims 16 recites, "if at least one first network condition is met,....if at least one second network condition is met,...if at least one third network condition is met…". There is an antecedent basis for these terms and are unclear what are these one first, one second and one third network conditions are referred to?

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-10, 14, 16, 18-21, 45 and 46 are rejected under 35 U.S.C. 101 because the claimed invention is directed to nonstatutory subject matter.

The claim is drawn to a "computer readable medium" comprising stored data. The specification is silent regarding the meaning of this term. Thus, applying the broadest reasonable interpretation in light of the specification [0024] and taking into account the meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art (MPEP §2111), the claim as a whole covers a transitory signal, which does not fall within the definition of a process, machine, manufacture, or composition of matter.

Applicant can overcome the rejection by introducing the phrase, “non-transitory” storage medium into the claims.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. As to claims 1, 2, 10, 14, 16, 18-22, 27 and 40-42 are rejected under 35 U.S.C 103(a) as being unpatentable over Ayyagari et al (Pub No.: US 2002/0176366 A1), hereinafter "Ayyagari", in view of Mayer, (Pub. No.: US 2002/0178246 A1), hereinafter "Mayer".

10. As to claim 1, Ayyagari discloses, acquiring at least one network attribute, (Ayyagari, [0006], where acquiring an ad hoc network under IEEE 802.11 is a network attribute), each network attribute corresponding to an attribute of a computer network (Ayyagari, Fig.2, [0006], where connecting to an ad hoc network satisfy the corresponding network attribute and connecting device attribute);

generating a value for at least one derived network DNA component according to at least one derived network DNA component specification, each derived network DNA component corresponding to an attribute of the computer network (Ayyagari, [0006], where value of the derived network DNA component is an ID of an ad hoc network/derived network DNA component in accordance with the connecting network device e.g. wireless 802.11 a, b, g), and at least one of said at least one derived network DNA component specification referencing at least one of said at least one network attribute and processing by which the value of the derived network DNA component is generated from the referenced at least one network attribute (Ayyagari, [0006], Fig.3, Where derived network DNA component/ad hoc network referencing

network DNA attribute e.g. 802.0x and processing a Network ID e.g. SSID is generated according to the network attribute); and

determining a network DNA for the computer network, the network DNA classifying the computer network (Ayyagari, [0006], where selection of network between ad hoc mode or infrastructure mode is determining a network DNA for computer network and using either of the network classifies the computer network), and the network DNA comprising at least one of said at least one derived network DNA component (Ayyagari, [0006], where acquiring an ad hoc network under IEEE 802.11 is a network attribute).

initiating on the computer connected to the computer network an execution of a network DNA policy action of the network DNA policy, the execution of the network DNA policy action configuring network security settings of the computer for a connection to the computer network when the network DNA policy condition of the network DNA policy is satisfied (Ayyagari, Fig.4, [0041], discloses a controlling logic to determine when, how and to whom a wireless user connects from the competing wireless networks available at any given time and place. The system uses a much detailed criteria to make the connection decisions based on configuration information e.g. service or network provider, signal strength, authentication process, operating profiles and policies set by user or employer or provider. Policies can be such as preferred network connection configuration in all the major cities in, therefore when computer detects the network it executes the corresponding network policies and upon satisfying the connection criteria authentication is granted to connect to the network).

Ayyagari however is silent on disclosing explicitly, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component and the network DNA policy condition is satisfied when the referenced derived network DNA component has a value specified in the network DNA policy; and

An execution of a network DNA policy action of the network DNA policy if the network DNA policy condition of the network DNA policy is satisfied.

Mayer however discloses, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component (Mayer, Fig.2, [0015], where analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology which relates to network DNA policy condition referencing network DNA component and further as disclosed in [0033], In step 245, the analysis platform determines whether a violation of the network policy has been detected. If so (Yes in step 245), the violation is recorded in step 250 and the process continues to step 255. Otherwise (No in step 245), the process continues to step 255); and

an execution of a network DNA policy action of the network DNA policy, the execution of the network DNA policy action configuring network security settings of the computer for a connection to the computer network when the network DNA policy condition of the network DNA policy is satisfied (Mayer, Fig.2, where the analysis platform receives the network policy as an input and then analyzes the network

configuration model to verify that the IP traffic from and to these hosts are limited according to the type of service, and to ensure that the right type of IP traffic get from/to a host, which includes the configuration of relevant routers for switching traffic, firewalls for passing through or dropping traffic, and local access control mechanisms on the host (e.g., TCP wrappers) for making the services accessible, further as disclosed in [0033], In step 245, the analysis platform determines whether a violation of the network policy has been detected. If so (Yes in step 245), the violation is recorded in step 250 and the process continues to step 255. Otherwise (No in step 245), the process continues to step 255, where violation of network policy is equivalent and within the scope of violation of network security setting).

Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari with the teachings of Mayer in order to provide a platform analyzer to simulate network configuration model according to the network policy and adds an entry to its final report each time that it detects a violation against the network policy in the network configuration model. The data in the entries pinpoints the cause of the deviation(s) from the network policy.

11. As to claims 16 and 22, Ayyagari and Mayer discloses the invention substantially as applied to claim 1 above, additionally, acquiring at least one attribute of the computer network (Ayyagari, Abstract, After detecting network access data, the device driver notifies the connection manager.);

generating a network species component according to a derived network DNA component specification, the network species component specification referencing at

least one attribute of the computer network (Ayyagari, Fig.5, [0014], with zero configuration a selection /generation of an appropriate network interface /network DNA from available networks is based on selection criteria which is equivalent to a network species component e.g. speed, interface type, cost metrics etc. further these attribute represents corresponds to the associated network species e.g. available networks);

determining a network DNA of the computer network, the network DNA comprising the network species component, (Ayyagari, Fig.5, Abstract, where determining to connect to one of the competing networks available defines the network DNA and specific setting to each of the network defines the species component);

the network species component indicating the network species classification selected from among a plurality of network species classification, the plurality of network species classification including an enterprise network, a home network, and a public network (Ayyagari, [0045], where sys tray icon contains the available plurality of networks which is same as network species classification and [0035] which incorporates, "just works" user experience, which greatly enhances the ability to realize the benefits of true nomadic computing. In this way, a wireless computer user may work on an established network at home, at work, in transit, at the airport, in a hotel which is a public network, etc.), the network species component indicating the network species is enterprise network if at least one first network condition is met, the network species component indicating the network species is home network if at least one second network condition is met, and the network species component indicating the network species is public place network if at least one third network condition is met (Ayyagari,

Fig.5, [0036], where using a zero configuration system within itself determines according to the policies setup without user intervention and so zero configuration recognizes the network species by determining whether user is at home “first condition”, at work "second condition”, in transit, at the airport or in a hotel “third condition” with available network e.g. WAN GPRS, 802.1x, WLAN 2, STA and this implementation is defined in [0035] which incorporates, "just works" user experience, which greatly enhances the ability to realize the benefits of true nomadic computing. In this way, a wireless computer user may work on an established network at home, at work, in transit, at the airport, in a hotel, etc., and may form ad hoc wireless networks with other wireless users all without having to manually reconfigure or adjust network variable settings to enable association with the different network types).

12. As to claim 2, is rejected under for same rationale as applied to claim 16 above.

13. As to claim 10, carry similar limitation as parent claim1 and therefore, is rejected under for same rationale.

14. As to claim 14, Ayyagari and Mayer discloses the invention substantially, including, wherein the network DNA policy reduces a probability of security vulnerability when switching between computer networks (Ayyagari, [0041], zero configuration system reduces the security vulnerability by providing a controlling logic to determine when, hoe and to whom a wireless user connects from the available wireless networks at any given time and place.

15. As to claims 21 and 27, Ayyagari and Mayer discloses the invention substantially as in parent claims 16 and 22, including, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component (Mayer, Fig.2, [0015], where analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology which relates to network DNA policy condition referencing network DNA component); and

initiating on the computer connected to the computer network an execution of a network DNA policy action of the network DNA policy, the execution of the network DNA policy action configuring network security settings of the computer for a connection to the computer network when the network DNA policy condition of the network DNA policy is satisfied (Ayyagari, Fig.4, [0041], discloses a controlling logic to determine when, how and to whom a wireless user connects from the competing wireless networks available at any given time and place. The system uses a much detailed criteria to make the connection decisions based on configuration information e.g. service or network provider, signal strength, authentication process, operating profiles and policies set by user or employer or provider. Policies can be such as preferred network connection configuration in all the major cities in, therefore when computer detects the network it executes the corresponding network policies and upon satisfying the connection criteria authentication is granted to connect to the network).

16. As to claims 18 and 42, Ayyagari and Mayer discloses the invention substantially as in parent claim 16, including, wherein the network DNA further comprises a network name component (Ayyagari, [0012], where SSID is a network name component), a network cost component (Ayyagari, [0014], where cost metrics are network cost component) a core access component (Ayyagari, [0012], where 802.1x is equivalent to core accessing component), a core addressing component (Ayyagari, [0012], where connecting via 802.1x means there is an IP addressing in place which is a core addressing component), a network security component (Ayyagari, [0012], where 802.1x authentication is a network security component) and a network technology component (Ayyagari, [0012], where ad hoc or infrastructure mode is a network technology component).

17. As to claim 19, Ayyagari and Mayer discloses the invention substantially as in claim 18 above, including, wherein the network technology component comprises at least one network operational attribute (Mayer, [0008], where VPN is a network operational attribute).

18. Claims 20, 40-41 carry similar limitations as claim 16 and 22 above and therefore are rejected under for same rationale additionally it is known that computer network comprises of security, network management and addressing attribute.

19. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ayyagari and Mayer as applied to claim 1 above in view of Anderson et al. (Pub. No.: US 2004/0068582 A1), hereinafter “Anderson”.

20. As to claim 3, Ayyagari and Mayer discloses the invention substantially as applied to claim 1 above, including, wherein at least one of said at least one derived network DNA component specification comprises at least one value of at least one of said at least one network attribute.

Ayyagari and Mayer however are silent on, “a linear transformation”.

Anderson however discloses, "a linear transformation" (Anderson, [0186], where network confidence level is Network DNA component is calculated based on linear combination of each of constituent confidence factor field).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari and Mayer with the teachings of Anderson in order to provide a hierarchy of network DNA with respect to network DNA confidence level which will help developing network architectural models in future.

21. As to claim 4, Ayyagari and Mayer and Anderson discloses the invention substantially, including, wherein said at least one derived network DNA component specification comprises a combination of said at least one network attribute (Anderson, [0186], where confidence factors are combination of raw and derived network DNA).

22. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ayyagari and Mayer in view of Beadles et al. (Patent No.: US 7159125 B2), hereinafter “Beadles”.

23. As to claim 5, Ayyagari and Mayer disclose the invention substantially as in parent claim 1 above. Ayyagari and Mayer however is silent on disclosing, "wherein at least one of said at least one derived network DNA component specification comprises a structured query language statement".

Beadles however, discloses, "wherein at least one of said at least one derived network DNA component specification comprises a structured query language statement" (Beadles, Col.7, lines 5-6, where Network policy store/Network DNA is implemented as SQL server database, further these policy's can be written in any other well known languages in the art e.g. pearl, Visual basic etc.).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari and Mayer with the teachings of Beadles in order to provide device management policy to have control over network via developing a policy to associated network devices.

24. As to claim 6, Ayyagari and Mayer and Beadles discloses the invention substantially including, derived network DNA component specification comprises an object oriented language statement (Beadles, Col.3, lines 10-14, The CIM which is also defined by the DMTF is a standard object-oriented model that represents objects in terms of instances, properties, relationships, classes and subclasses).

25. As to claim 7, Ayyagari and Mayer and Beadles discloses the invention substantially including, derived network DNA component specification comprises a scripting language statement (Beadles, Col.3, lines 10-14, where enforcing the policy

requires the batch / "scripting language" or calling a function which is also embedded / linked within the function or program).

26. As to claim 8, Ayyagari and Mayer and Beadles disclose the invention substantially as in claim 5-7 above, including, wherein acquiring at least one network attributes comprises acquiring a plurality of network attributes specified by the acquisition priority list comprising at least a subset of a domain name, one or more IP addresses, verified presence of network infrastructure elements, parameters received from a network server, a communications media type, a service provider, a nominal available communication bandwidth, a measured available communications bandwidth, logical network location and physical network location (Beadles, NAT Directory schema, Col.23 and 24, Abstract, where multiple hierarchical services which are plurality of network DNA components and from hierarchy may priorities can be extracted e.g. reliability, security, confidence level etc. Further it will be obvious to make the hierarchy based policy as per organizational or user specific preferences).

27. As to claim 9, carry similar limitations as claim 8 above, additionally Beadles discloses the limitation "ordered set of network DNA policies that references the plurality of network attribute (Beadles, Col.27 "device XML Schema" and Col.29, lines 1-7, In one embodiment, the directory is navigated to gather the information needed to populate the device XML schema so it can be stored in the Configuration Store for later retrieval and application by the various Device Plugs-Ins (DPIs). The NAT configuration consists of defining interfaces and processing rules and Col.17, lines 58-67, where XML

schema comprises of three ordered set of network DNA policy Conditions include Custom Conditions, Fully Meshed Conditions, and Hub Spoke Conditions and processing requires some structuring of the calls that defines the attributes).

28. Claims 23, 25-26, 28-37 and 45 are rejected under 35 U.S.C 103 (a) as being unpatentable over Ayyagari and Mayer in views of Williams et al. (Pub. No.: US 2005/0257267 A1), hereinafter "Williams".

29. As to claim 31, Ayyagari and Mayer disclose the invention substantially as in claim 1 and 27 above, including, testing network policy condition (Mayer, [0015], The analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology).

Ayyagari and Mayer however are silent on disclosing explicitly, whether sufficient network DNA referenced by the DNA network policy condition of the network DNA policy has been acquired.

Williams however discloses, whether sufficient network DNA referenced by the DNA network policy condition of the network DNA policy has been acquired (Williams, [0099], where testing one of the selected policy from test menu implies testing different policy to see if acquired data is sufficient).

Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari and Mayer with the

teachings of Williams in order to provide a network auditing system for auditing the security of a data communications network.

30. As to claim 23, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 22, including, wherein said at least one network DNA store comprises a current network DNA store and a network DNA history store (Ayyagari, Abstract, where profile setting is a DNA history store as it is predefined settings and to determine which network to connect among available networks is current network DNA store).

31. As to claim 25, carry similar limitations as parent claim 22, therefore is rejected under for same rationale.

32. As to claim 26, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 22, including, wherein each network DNA policy comprises a derived network DNA components dependency list that lists each derived network DNA component of the network DNA referenced by the network DNA policy (Williams, [0072, lines 1-6], where policy library-42 is a repository of pre-established policies, therefore it is obvious that any network build on these policies will be derived and dependent on these policies).

33. As to claim 28, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if an expression specified by the network DNA policy condition evaluates to Boolean true (Williams, Fig.12A, policy violation-916, [0135],

where complying with the policy is “Boolean true”, which handle the violation per policy instruction).

34. As to claim 29, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if an expression specified by the network DNA policy condition evaluates to Boolean false (Williams, Fig.12A, policy violation-916, [0135], where not complying with the policy in false, which terminates the process).

35. As to claim 30, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if evaluating an expression specified by the network DNA policy condition results in an evaluation error (Williams, [0068], where policy evaluation is tested before deployment, which obviously is an essential step of removing any remaining errors in policy).

36. As to claims 32 and 45, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 27, including, each network DNA component is associated with a confidence level (Williams, Fig.3, recommendation engine, [0078], where recommendation engine is provide a confidence level and each policy is associated with confidence level); and

sufficient network DNA has been acquired for the network DNA policy if the confidence level of each network DNA component referenced by the network DNA

policy condition of the network DNA policy is greater than zero (Williams, [0144], where mapping score is above a given threshold and where threshold can be a zero).

37. As to claim 33-34, carry similar limitation as claim 32 above and therefore, are rejected under for same rationale.

38. As to claim 35, is rejected under for same rationale as applied to claims 16 and 22 above.

39. As to claim 36, Ayyagari, Mayer and Williams disclose the invention substantially as in parent claim 35, including, wherein the network DNA generator is further, at least, configured to maintain at least one derived-raw network DNA component dependency list (Ayyagari, [0045], where list of compatible "FH or DS" SSIDs visible in infrastructure mode is maintained which is same as derived-raw network DNA component dependency list), said at least one derived-raw network DNA component dependency list comprising, for each derived network DNA component generated by the network DNA generator, a list referencing each raw network DNA component referenced by each derived network DNA component specification associated with the derived network DNA component (Ayyagari, [0045], where network interface/DNA generator on “sys tray” in the windows environment provides the configuration details of available/raw network list and each network icon represents the association with the derived network DNA component).

40. As to claim 37, is rejected under for same rationale as applied to claim 36 above. Additionally, Ayyagari discloses, the derived network DNA refresh list referencing each derived network DNA component dependent upon a changed raw network DNA component (Ayyagari, [0046], selecting a particular SSID from the displayed list would enable the STA to force a transition out of Ad Hoc mode and restart / refreshing the association mechanism per IEEE 802.11 usage mode specified by the authentication option discussed above.).

41. Claims 38-39 are rejected under 35 U.S.C 103(a) as being unpatentable over Ayyagari and Mayer as applied to claim 22 above in view of Britt et al. (Patent No.: 6,675,209 B1), hereinafter "Britt".

42. As to claim 38, Ayyagari and Mayer discloses the invention substantially as in parent claim 22 above, including, "acquiring a plurality of raw network DNA component" (Ayyagari, [0045], where network interface on the "sys tray" acquires the plurality of available networks). Ayyagari and Mayer however are silent on disclosing explicitly, "acquirer, acquire network DNA component according to priority list specified by raw network DNA acquisition priority list" or "each raw network DNA component corresponding to an attribute of said at least one computer network".

Britt however discloses, "acquirer, acquire network DNA component according to priority list specified by raw network DNA acquisition priority list" (Britt, Claim 16) or "each raw network DNA component corresponding to an attribute of said at least one computer network" (Britt, Claim 16).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari and Mayer with the teachings of Britt in order to provide an adaptive system module includes a network organizer that categorizes the multiple segments of the network, a network prioritizer that ranks the categorized segments amongst themselves according to a necessity to obtain data traffic information for analysis, and a system optimizer that determines how many of the ranked segments can provide data traffic information within a set protocol data unit ("PDU") credit limit.

43. As to claim 39, is rejected under for same rationale as applied to claim 38 above.

44. Claims 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ayyagari and Mayer as applied to claims 40 and 41 above in view of Anderson et al. (Pub. No.: US 2004/0068582 A1), hereinafter "Anderson".

45. As to claim 43, Ayyagari and Mayer disclose the invention substantially as in parent claim 40. Ayyagari and Mayer however are silent on disclosing explicitly, "wherein the network DNA further comprises a confidence level for each of the at least one network classification component".

Anderson however, discloses, "wherein the network DNA further comprises a confidence level for each network classification component" (Anderson, Fig.28, [00196], where fuzzy and crisp logic with confidence level is disclosed).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Ayyagari and Mayer with the

teachings of Anderson in order to provide a hierarchy of network DNA with respect to network DNA confidence level which will help developing network architectural models in future.

46. As to claim 44, Ayyagari, Mayer and Anderson discloses the invention substantially as in parent claim 40 above, including, at least one value of at least one of the network classification component is determined probabilistically (Anderson, [0196], where network address is located probabilistically); and the confidence level of said at least one of at least network classification component determined probabilistically corresponds to a margin of error in the determination (Anderson, Fig.28, [0196], where probability means result is based on margin of error).

Allowable Subject Matter

47. Claims 46 and 47 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Reasons for Allowance

48. Prior art of record alone or in combination does not teaches the limitations among other things, determining the network species is enterprise network if the first network condition is met, the first network condition being met if a plurality of:

(a) the computer network is a secure network and is a managed network,

(b) the computer network is a private network, and

(c) the computer network provides connectivity to one or more specified enterprise resources;

determining the network species is home network if the second network condition is met, the second network condition being met if a plurality of:

(a) the computer network is an insecure network and an unmanaged network,

(b) the computer network provides ad hoc and/or limited connectivity between network nodes and other computer networks,

(c) the computer network is a private network, and

(d) the computer network is a premise network or a proximity network; and

determining the network species is public place network if the third network condition is met, the third network condition being met if a plurality of:

(a) the computer network is an insecure network and an unmanaged network,

(b) the computer network has an associated access cost, and

(c) the computer network is not a private network, is not a premise network and is not a proximity network.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TAUQIR HUSSAIN whose telephone number is (571)270-1247. The examiner can normally be reached on 7:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thu Nguyen can be reached on 571 272 6967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. H./
Examiner, Art Unit 2452

/THU NGUYEN/
Supervisory Patent Examiner, Art Unit 2452